WHAT IS CLAIMED IS:

1. A secure communication system, comprising:

a first communication station;

a secure communication signal generated at a first communication station;

a second communication station coupled to said first communication station, said second communication station being effective to receive said secure communication signal;

said second communication station being operable to verify a content of said secure communication signal and generate a verified secure communication signal; and

a third communication station coupled to said second communication station, said third communication station being effective to receive said verified secure communication signal.

2. A secure communication system according to claim 1, further comprising:

a sender public/private key pair;

a first unique authentication signal related to said content and said sender private key from said sender public/private key pair; and

said secure communication signal further comprises said first authentication signal.

3. A secure communication system according to claim 2, further comprising:

a first random encryption key provided at said first communication station;

a first encryption engine operable to process at least one of said content and said sender public key from said sender public/private key pair with said first random encryption key to provide an encrypted communication signal; and

said secure communication signal comprises said encrypted communication signal.

4. A secure communication system according to claim 3, further comprising:

a system public/private key pair;

said encryption engine being further operable to process said first random encryption key with said system public key from said system public/private key pair to provide a first encrypted random key; and

said secure communication signal further comprises said first encrypted random key.

5. A secure communication system according to claim 2, further comprising:

a volatile memory storage at said first communication station; and

said sender public/private key pair extant in said volatile memory storage.

6. A secure communication system according to claim 5, further comprising:

a public/private key pair generator having an input;

a user selectable code suitable for application to said input of said public/private key pair generator; and

said sender public/private key pair being an output of said public/private key pair generator and being related to said user selectable code.

7. A secure communication system according to claim 6, further comprising:

an individual specific code generator device;

said code generator device operable to process a characteristic of an individual to provide said user selectable code.

8. A secure communication system according to claim1, further comprising:

an electronic messaging program operable with said first communication station; and

a secure electronic messaging program operable with said electronic messaging program to accept input therefrom and provide said secure communication signal.

9. A secure communication system according to claim 8, further comprising:

an option selection program for said secure electronic messaging program; and

said option selection program provides selectable options accessible to permit a user to select options related to operation of said secure electronic messaging program.

10. A secure communication system according to claim 9, wherein said option selection program is a portion of an installation program operable to install said secure electronic messaging program in at least one of said first and third communication stations.

11. A secure communication system according to claim 9, wherein said selectable options include at least one of an option for storing or not storing a sender private key from a sender public/private key pair and an option for entry of a pass code.

12. A secure communication system according to claim 9, wherein:

said selectable options include control options for controlling aspects of said secure communication signal; and

said control options including at least one of whether a virus should be passed with a said secure communication or not, whether said content should be stored or not and whether said first authentication signal should be stored or not.

13. A secure communication system according to claim 1, further comprising:

an electronic sender address identifying a user at said first communication station;

an electronic station address identifying said second communication station; and

said secure communication signal is addressed from said sender address

to said station address.

14. A secure communication system according to claim 13, further comprising:

at least one electronic receiver address identifying a user at said third communication station; and

said verified secure communication signal is addressed from said station address to said at least one receiver address.

15. A secure communication system according to claim 1, further comprising:

an electronic station address identifying said second communication station;

at least one electronic receiver address identifying a user at said third communication station; and

said verified secure communication signal is addressed from said station address to said at least one receiver address.

16. A secure communication system according to claim 2, further comprising:

a hashing engine coupled to said first communication station;

said hashing engine being operable to process said content to provide a hash code; and

a combination of said hash code and said sender private key from said sender public/private key pair provides said first authentication signal.

17. A secure communication system according to claim 1, wherein said first communication station further comprises a hash code generator;

said hash code generator being operable to generate a hash code related to said content;

a sender private key from a sender public/private key pair;

said hash code and said sender private key being combined to provide a first authentication signal; and

said secure communication signal further comprises said first authentication signal.

18. A secure communication system according to claim 1, wherein said second communication station further comprises a chronometric indicia mechanism being operable to provide chronometric indicia suitable for insertion in said content, whereby a time and date of receipt of said secure communication signal at said second communication station can be indicated in said verified secure communication signal.

19. A secure communication system according to claim 1, wherein said second communication station further comprises a virus checking engine;

said virus checking engine being operable to scan said content for software viruses; and

a result of said scan provides said verification of said content.

20. A secure communication system according to claim 19, wherein said virus checking engine is further operable to scan said secure communication signal for software viruses and remove a virus detected by said

scan.

21. A secure communication system according to claim 2, wherein said verification is based on said first authentication signal.

22. A secure communication system according to claim 1, further comprising:

a system public/private key pair;

a second unique authentication signal related to a content of said verified communication signal and said system private key from said system public/private key pair; and

said verified secure communication further comprises said second authentication signal.

23. A secure communication system according to claim 2, further comprising:

a system public/private key pair;

a second unique authentication signal related to a content of said verified communication signal and said system private key from said system public/private key pair; and

said verified secure communication further comprises said second unique authentication signal.

24. A secure communication system according to claim 1, further comprising:

a random encryption key provided at said second communication

station;

an encryption engine operable to process at least one of a content of said verified secure communication signal and a system public key from a system public/private key pair with said random encryption key to provide an encrypted verified communication signal; and

said verified secure communication signal comprises said encrypted verified communication signal.

25. A secure communication system according to claim 3, further comprising:

a second random encryption key provided at said second communication station;

a second encryption engine operable to process at least one of a content of said verified secure communication signal and a system public key from a system public/private key pair with said second random encryption key to provide an encrypted verified communication signal; and

said verified secure communication signal comprises said encrypted verified communication signal.

26. A secure communication system according to claim 24, further comprising:

a recipient public/private key pair;

said encryption engine being further operable to process said random encryption key with said recipient public key from said recipient public/private key pair to provide an encrypted random key; and

said verified secure communication signal comprises said encrypted

random key.

27. A secure communication system according to claim 25, further comprising:

a recipient public/private key pair;

said second encryption engine being further operable to process said second random encryption key with said recipient public key from said recipient public/private key pair to provide an encrypted random key; and

said verified secure communication signal comprises said encrypted random key.

28. A secure communication system according to claim 26, wherein said recipient public/private key pair is provided by a public/private key pair generator based on an input user selectable code.

29. A secure communication system according to claim 27, wherein said recipient public/private key pair is provided by a public/private key pair generator based on an input user selectable code.

30. A secure communication system according to claim 1, further comprising:

a firewall at said second communication station;

said firewall operable to at least one of block unauthorized communications, detect viruses and remove viruses.

31. A secure communication system according to claim 1, further

comprising:

a volatile memory storage at said second communication station; and

said content of said secure communication signal extant in said volatile memory storage.

32. A secure communication system according to claim 1, further comprising:

a return receipt issued by said second communication system; and

said return receipt indicates receipt of said verified secure communication signal at said third communication station.

33. A secure communication system according to claim 1, further comprising:

a load balancer at said second communication station;

said load balancer coupled to a plurality of system nodes; and

said load balancer can determine processing loads on said system nodes, whereby said secure communication signal can be routed to an appropriate system node to facilitate efficient processing.

34. A secure communication system according to claim 1, further comprising:

a database coupled to said second communication station; and

said database provides a cross reference between sender public/private key pairs or between subscriber identifying information and a subscriber public key.

35. A secure communication system according to claim 1, further comprising:

a record of secure communication transactions; and

a reporting engine operable to provide reports related to said record.

36. A secure communication method, comprising:

securing a message at a first location;

transmitting said secure message to a second location;

receiving said secure message at said second location;

verifying a content of said secure message at said second location; and

transmitting said verified, secure message to a third location.

37. A secure communication system, comprising:

a sending device effective to originate an electronic message;

a security producing operator coupled to said sending device and operable to produce a secure message based on said electronic message;

a communication network coupled to said sending device, said communication network operable to transmit said secure message;

a central processor coupled to said communication network and effective to receive said secure message from said communication network;

said central processor being operable to verify a content of said secure message;

said central processor being further operable to transmit said verified secure message to said communication network;

a receiving device coupled to said communication network and operable to receive said verified secure message from said communication network; and

a security removing operator coupled to said receiving device and operable to reproduce said electronic message from said verified secure message.

38. A secure communication system, comprising:

a sending device;

a receiving device;

a transmission medium;

a security mechanism coupled to each of said sending and receiving devices; and

said security mechanism being operable to transform at least one of a secure message and an unsecure message to an unsecure message and secure message, respectively, whereby said sending and receiving devices can communicate unsecure messages originating from at least one of said sending and receiving devices as secure messages over said transmission medium, and said security mechanism being further operable to provide authentication of said secure messages.

39. A method for secure communication, comprising:

operating on an unsecure transmission signal to produce a secure transmission signal including an authenticating code;

transmitting said secure transmission signal;

receiving said secure transmission signal;

operating on said secure transmission signal to produce said unsecure transmission signal; and

verifying said received unsecure transmission signal using said authenticating code.

40. A method for secure communication, comprising:

operating on an unsecure transmission signal at a sender to produce a secure transmission signal;

transmitting said secure transmission signal to a verification operator;

receiving said secure transmission signal at said verification operator;

operating on said secure transmission signal at said verification operator to verify a content of said secure transmission signal;

transmitting said verified secure transmission signal to a receiver;

receiving said verified secure transmission signal at said receiver; and

operating on said verified secure transmission signal at said receiver to produce said unsecure transmission signal.

41. A secure communication system, comprising:

an encryption/decryption operator coupled to a plurality of communication devices;

said plurality of communication devices coupled together across a communication medium;

said encryption/decryption operator including an encryption/decryption code generator;

said encryption/decryption operator is effective to transform unsecure communications to secure communications and vice-versa through application of an encryption/decryption code provided by said encryption/decryption code generator; and

at least one of said communication devices is configured with:

an input to receive said secure communications;

said encryption/decryption operator effective to transform said received secure communications to received unsecure communications;

a verification processor operable to verify a content of said received unsecure communications in combination with said encryption/decryption code;

said encryption/decryption operator effective to transform said verified unsecure communication to a verified secure communication; and

an output to transmit said verified secure communication to at least one other communication device.

42. A method for secure communication, comprising:

generating a random encryption key;

encrypting a communication signal with said random encryption key;

encrypting said random encryption key;

transmitting a secure communication signal comprising said encrypted communication signal and said encrypted random encryption key;

receiving said secure communication signal;

decrypting said random encryption key;

decrypting said encrypted communication signal with said random encryption key; and

verifying a content of said received, decrypted communication signal.